Math200B - HW #1

Jay Ser

2026.01.16

1.

(a)

Suppose D is a Bezout domain. Take $a, b \in D \setminus 0$. Then $\exists d \in D$ such that $\langle a, b\rangle = \langle d\rangle$. $\langle a\rangle \subset \langle d\rangle \implies d \mid a$, and similarly, $d \mid b$. By definition of d, $d \in \langle a, b\rangle$, which proves the forward direction.

Next, suppose for arbitrary $a, b \in D \setminus 0$, $\exists d \in D$ such that $d \mid a$, $d \mid b$, and $d \in \langle a, b\rangle$. The divisibility condition says $\langle a, b\rangle \subset \langle d\rangle$. Vice versa, $d \in \langle a, b\rangle \implies \langle d\rangle \subset \langle a, b\rangle$. So for arbitrary $a, b \in D \setminus 0$, $\exists d \in D$ such that $\langle a, b\rangle = \langle d\rangle$. Of course, if $a = 0$, then $\langle a, b\rangle = \langle b\rangle$. This shows D is a Bezout Domain.

(b)

Induct on n, the number of elements generating $I \lhd D$. If $n = 1$, I is a principal ideal by definition. Suppose ideals generated by at most $n - 1$ elements are principal and let

$$I = \langle a_1, a_2, \ldots, a_n\rangle$$

for some $a_1, \ldots, a_n \in D$. $\langle a_1, \ldots, a_{n-1}\rangle \subset I$, and by the inductive hypothesis, $\exists d \in D$ such that

$$\langle d\rangle = \langle a_1, a_2, \ldots, a_{n-1}\rangle$$

Namely, since $d \in \langle a_1, \ldots, a_{n-1}\rangle$, $d \in I$. Thus $I = \langle d, a_n\rangle$. Since D is a Bezout Domain, $\exists d' \in D$ such that

$$\langle d'\rangle = \langle d, a_n\rangle = I$$

This shows I is principal.

(c)

The forward direction is trivial. Suppose D is a UFD and a Bezout Domain and take any $I \lhd D$. Since D is a UFD, every element of I has a unique prime factorization. Let $a \in I$ be an element that has the least number of (not necessarily distinct) prime factors. Note that such an element is unique up to associates: suppose

$$a = up_1p_2 \cdots p_n, \quad a' = vq_1q_2 \cdots q_n$$

are factorizations of two nonassociate elements of I with the least number of prime factors. Then their greatest common divisor has strictly less prime factors than a_1 and a_2. Because D is a Bezout Domain, the greatest common divisor is in I, contradicting the assumption on a and a'.

Now, take any $b \in I$. Let $d \in D$ be the element satisfying $\langle d\rangle = \langle a, \rangle$. Because d divides a, d has at most the number of prime factors that a has. But $d \in \langle a, b\rangle \subset I$. Thus, by the assumption on a, d has the exact same prime factors as a, i.e.,

$$\langle d\rangle = \langle a\rangle \subset \langle a, b\rangle = \langle d\rangle$$

which shows $\langle a\rangle = \langle a, b\rangle$. Since this holds for all $b \in I$, one concludes $I = \langle a, b\rangle$.

2.

In the ring $A = \mathbb{Q}[x, xy, xy^2, \ldots]$, the chain

$$\langle x \rangle \subset \langle x, xy \rangle \subset \langle x, xy, xy^2 \rangle \subset \ldots$$

is a strictly increasing chain because no power of y is in A. Thus A is not Noetherian.

3.

(a)

Since r/s is a root, the following equality holds:

$$-a_0 = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \ldots + a_1(r/s)$$

Multiplying both sides by s^n,

$$-s^n a_0 = a_n r^n + a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + \ldots + a_1 r s^{n-1}$$

s divides the left hand side, and s divides all the terms on the right hand side except $a_0 r^n$, so $s \mid a_0 r^n$. s and r share no prime factors, so $s \mid a_0$. Similarly, r divides the right hand side, and r and s share no common prime factor, so $r \mid a_0$.

(b)

Suppose $r/s \in D$. Then $f(x) := x - r/s \in D[x]$ is a monic polynomial with r/s as a root.

Conversely, suppose $f(x) := a_n x^n + \ldots + a_0 \in D[x]$, where $a_n = 1$, has r/s as a root. If $s \nmid r$, then define

$$d := \gcd(r, s), \quad r' := r/d, \quad s' := s/d$$

d is nonassociate to s, so s' is nonunit. $f(r'/s') = 0$, so $s' \mid a_0 = 1$ by the previous problem. This is a contradiction, so s must divide r.

(c)

Denote $R = \mathbb{Z}[2\sqrt{2}]$. Consider $f(x) = x^2 - 2 \in R[x]$. $\sqrt{2} = \frac{2\sqrt{2}}{2}$ is a root of $f(x)$ and its numerator and denominator is in R, but $\sqrt{2}$ itself is not in R. By part (b), R is not a UFD.

4.

5.

6.

7.

Suppose $p = (a+bi)(c+di)$, where $a+bi$ and $c+di$ are not units. Using the fact that the norm function on $\mathbb{Z}[i]$ is multiplicative, obtain

$$p^2 = (a^2+b^2)(c^2+d^2)$$

Since the two factors of p are not units and the norm function maps to $\mathbb{Z}_{\geq 0}$, it follows that $a^2+b^2 = c^2+d^2 = p$.

Next, suppose $\exists a, b \in \mathbb{Z}$ such that $a^2+b^2 = p$. Then

$$\begin{aligned} & b^2 && \equiv -a^2 && \pmod{p} \\ \implies & b^{-2}b^2 && \equiv -(b^{-1}a)^2 && \pmod{p} \\ \implies & (b^{-1}a)^2 && \equiv -1 && \pmod{p} \end{aligned}$$

where b^{-1} is guaranteed to exist because $\mathbb{Z}/p\mathbb{Z}$ is a multiplicative group. So the equation $x^2 \equiv -1 \mod p$ does indeed have a solution.

Finally, assume $b^2 \equiv -1 \mod p$ for some $0 < b < p$. Then $p \mid b^2+1 = (b-i)(b+i)$. Suppose p is irreducible in $\mathbb{Z}[i]$. Then p is prime in $\mathbb{Z}[i]$, so $p \mid (b-i)$ or $p \mid (b+i)$. Without loss of generality, suppose $p \mid b-i$. Write $pq = b-i$ for some $q \in \mathbb{Z}[i]$ that is not a unit. Norming both sides, obtain

$$ap^2 = b^2+1$$

where $a := \lambda(q) > 1$. This contradicts the assumption that $b < p$. So p is not irreducible in $\mathbb{Z}[i]$.

8.